Alerta de seguridad informática	**8FFR-00091-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**15 de Octubre de 2019**
Última revisión	**15 de Octubre de 2019**

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de **Banco Estado**, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL´s

https[://]www[.]sedfineosntas[.]space/inicio/index[.]html

Domain sedfineosntas.space

sedfineosntas / space / Subdomains

record type	TTL	value		
A	14400	192.185.186.244		
NS	86400	ns1.onixserver.com	Zones on DNS server	192.185.186.27
NS	86400	ns2.onixserver.com	Zones on DNS server	192.185.186.28
MX	14400	0 mail.sedfineosntas.space		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname	ns1.onixserver.com	
		Rname	onixhosting.gmail.com	
		Serial number	2019101202	
		Refresh	86400	
		Retry	7200	
		Expire	3600000	
		Minimum TTL	86400	

Ilustración 1 Dominio donde se Aloja Url del Banco Estado, Falso y DNS que utiliza

Certificado

Criteria	Identity = 'sedfineosntas.space'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
1940868483	2019-09-30	2019-09-30	2019-12-29	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1940868361	2019-09-30	2019-09-30	2019-12-29	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Estado

IP´s

192[.]185[.]186[.]244

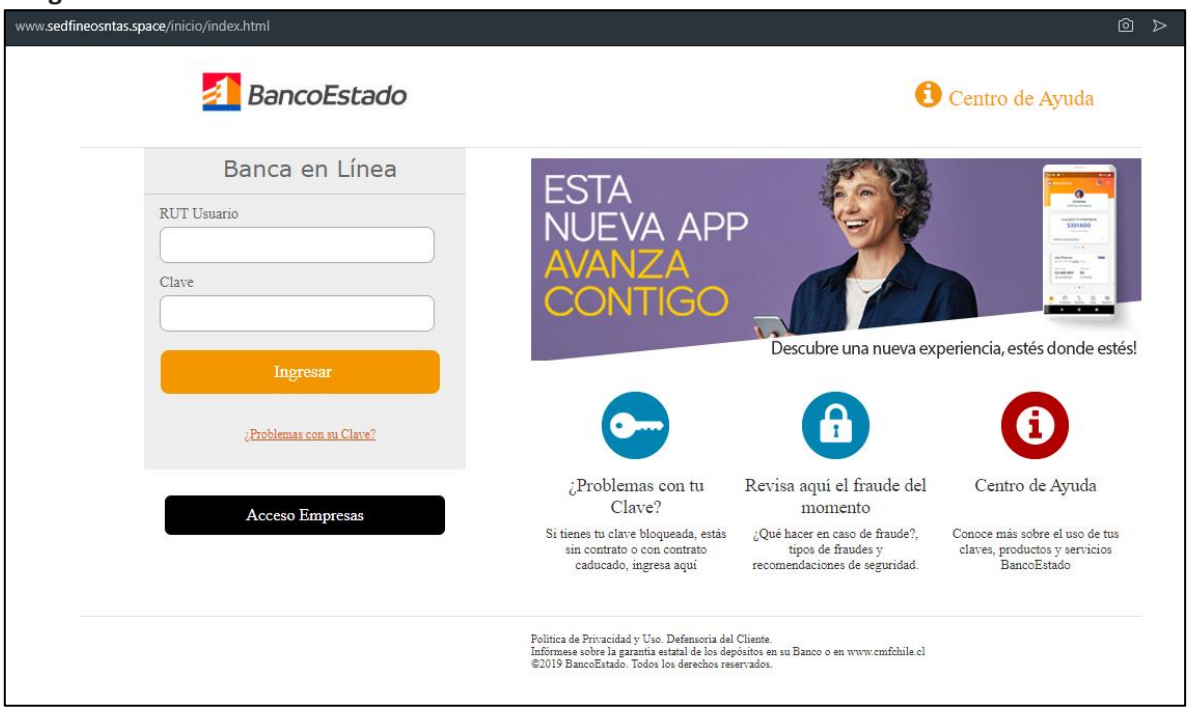
Domain sedfineosntas.space is located on IP address << 192.185.186.244 >>	
Block start	192.185.0.0
End of block	192.185.255.255
Block size	65536 Domains in block
Block name	HGBLOCK-10
AS number	46606
Parent block	192.0.0.0 - 192.255.255.255
Organization	WEBSITEWELCOME.COM
City	Houston
Region/State	Texas
Country	US , United States
Reg. date	2013-07-22
Host name	192-185-186-244.unifiedlayer.com
Web server	nginx/1.10.2

Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

Seattle, Washington, Estados Unidos

Imagen del sitio



Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido, hacia la URL maliciosa
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.15 10:11:09 -03'00'